VoIP Services with DDoS Mitigation over NFV Architectural Framework

陳嘉瑋 劉怡君 劉又聖 田蕙瑜 吳坤熹
國立暨南國際大學 資訊工程系
{s107321047,s107321014,s107321024,s107214005,solomon}@ncnu.edu.tw

摘要

在本篇論文中，我們將網路電話服務以 Network Function Virtualization(NFV)架構進行佈署，並提出自動化之防禦機制。使網路電話服務不再需要人力二十四小時看管。除此之外，將網路電話服務發展在 NFV 架構下，在重新佈署時會更加迅速且方便。我們模擬服務受到 DDoS 攻擊時，會如何判斷並進行防禦，防止服務受到影響。根據實驗結果，所提出的自動化防禦手段的確能有效且迅速的隔絕 DDoS 攻擊，在 45 秒內即可阻隔攻擊，將服務所受到的影響降至最低。

關鍵詞: DDoS、NFV、OpenStack。

1. 緒論

隨著近年來 5G 的興起，Network Function Virtualization(NFV)的技術也逐漸受到大家的重視。在傳統網路中，每一項網路服務都有屬於自己的硬體設備，像是:防火牆(Firewall)、路由器(Router)、入侵預防系統(Intrusion Prevention System，縮寫為 IPS)。NFV 的概念則是將這些網路服務定義成一個 Virtualized Network Function(VNF)，利用虛擬化的技術將這些網路服務整合在一群伺服器上，如此一來就能減少硬體的開銷，也容易維護。將傳統的服務進行虛擬化後，安全防護將更有彈性。由於整個資源都進行虛擬化的配置，所以在遭到攻擊時，管理者能夠自由的去決定該分配多少資源。在遭遇攻擊時，傳統的方式是必須手動開啟防禦機制，但在 NFV 架構下則可以動態分配資源並開啟防護機制。在 NFV 的架構下，虛擬化的技術讓網路的建置具有更高的擴充性與彈性。本篇論文的研究動機在於提出 NFV 中自動化防禦的架構，俾使實施防禦機制時能夠更加迅速以及更有效率。

1.1 研究目的

本篇論文是基於在網路電話服務虛擬化後，提出一種系統架構。此架構能夠偵測網路電話服務之品質，並判斷是否遭到攻擊。一旦遭到攻擊，則會自動地啟動防禦機制並通知管理員，將攻擊端與其他正常使用者進行隔離。在此虛擬化的架構下，能夠在不需人工手動操作下，啟動防禦機制，使網路電話伺服器能繼續服務；並在攻擊結束後將防禦時所佔用的資源自動釋放。

本篇論文共分為七節。第二節為研究背景;第三節為文獻探討;第四節敘述在 NFV 架構下的網路電話服務;第五節為系統實作;第六節為分析與比較;最後則是本篇論文的結論與未來展望。

2. 研究背景

此節介紹本篇論文之研究背景

2.1 SIP 通訊服務

作為通訊服務用的伺服器使用了對話啟動協定(Session Initiation Protocol，SIP)來提供網路電話通訊服務。SIP 為位於開放式系統互聯模型(Open System Interconnection Model，OSI 模型)網路應用層的控制協定，藉由多媒體會談(Multimedia Session)的建立(Initiate)、修改(Modify)與終止(Terminate)等控制信號 ，和多種協定偕同工作，以完成各式語音、影片、即時通訊等多媒體串流的互動式使用者對談，並可管理終端設備間彼此的連線狀態。SIP 通訊模式與超文本傳輸協定(HyperText Transfer Protocol，HTTP)相仿，採用請求(Request)、回應(Response)模式，並提供數種要求命令(Command)和回應碼(Status Code)，配合表頭欄位(Header Fields)和通訊內文(Content)完成通訊控制。SIP 伺服器的運作模式如圖一所示：用戶代理(User Agent)會先向 SIP 伺服器發送註冊(REGISTER)的請求；當用戶代理間欲通話時，則會先發送邀請(INVITE)至 SIP 伺服器，再由伺服器轉傳給目標用戶代理。若該目標用戶代理接通電話，則其向 SIP 伺服器回傳回應碼 200 OK 接收通話請求，最後再由發起者回傳 ACK 代表通話建立成功；結束通話時可由任一方送出 BYE 的請求。

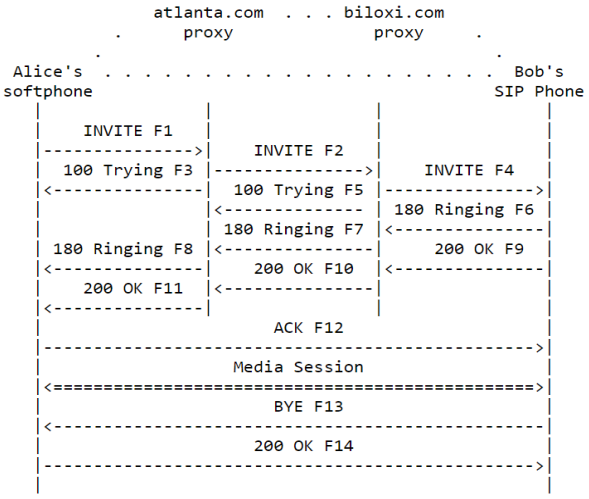

圖 1: SIP session setup example with SIP trapezoid [2]

2.2 DDoS 攻擊機制

Distributed Denial of Service(DDoS)，中文名為分散式阻斷服務攻擊，此網路攻擊手法為 Denial of Service (DoS，阻斷服務攻擊) 的延伸。在 DoS 中攻擊者會透過中斷目標伺服器連接到 Internet 的服務，使對方無法提供網路資源給其使用者。而 DoS 的實現方式，通常是由攻擊者向攻擊目標發送氾濫的網路請求封包，藉此消耗目標伺服器的網路頻寬、導致對方系統超載，並阻止來自合法使用者的請求封包獲得服務。而 DDoS 的攻擊方式即由多方攻擊來源同時向目標進行 DoS 攻擊，故名為「分散式」(distributed)阻斷服務攻擊。DDoS 名詞解釋可參閱 RFC 4732 [3]，其中提及了 DoS 與 DDoS 的定義以及常見之攻擊途徑。

隨著網路技術的發展，以單一來源進行攻擊的 DoS 愈來愈難以實現，因為被攻擊方在面對 DoS 時只需透過阻止單一的攻擊來源 IP 位址發送的氾濫封包便可以防止系統癱瘓，所以後來衍伸出了 DDoS 的攻擊方式，相比於 DoS 較不容易預防。在分散式的攻擊模式中，要如何偵測到並有效阻止來自多方攻擊來源傳送的封包，將會是一大難題。如何防禦 DDoS 攻擊之研究可參閱文獻[12][15][16]。

2.3 NFV

Network Function Virtualization (NFV)是一項可以將網路功能從專屬的硬體設備中抽離出來，並透過軟體去定義、執行這些功能的技術。就如同 SDN (Software-Defined Networking) 的技術將 Control Plane 和 Data Plane 抽離，NFV 的技術將軟體和硬體抽離。其目標在將許多網路設備的功能，像是處理網路安全的防火牆(Firewall)、入侵偵測系統(Intrusion Detection System)，以及增進效能的代理伺服器(Proxy)、網路快取(Cache)等，都能利用標準的硬體伺服器來執行。NFV 預期可達到以下優點:

(1) 減少在購買專屬功能硬體設備上的開銷

任何組織為了防護其區域網路，必然需要一些硬體設備(如: 防火牆)來做資安上的防護。而現今網路發展的速度非常地快速，很可能剛過兩三年這些設備的防護能力就已經不符需求，此時可能就需要重新添購專屬的防護設備。如果使用 NFV 來佈署防護功能，只要在初期購入標準的硬體設備，後續就能夠將許多不同的防護功能啟用在這台硬體設備上，而不必像過去一種防護功能就要單獨購買一台專屬設備，以此減少硬體購入上的開銷。

(2) 避免被硬體設備綁定系統架構

由於 NFV 上的網路功能皆為虛擬化，若管理者希望更新一個更好的防護功能，來取代現有的防護功能，在 NFV 的架構下只須把對應的軟體部分替換掉，硬體可以沿用原有的硬體伺服器。相較於舊式的架構必須把舊有的軟硬體一起替換掉，絕對容易多了；畢竟一個專屬功能的硬體設備通常價值不斐，很難說換就換。

(3) 動態調整資源配置

在 NFV 的技術中，所有的網路功能皆虛擬在 Virtual Machine (VM)上，這樣的好處是可依需求動態地調整資源配置。假設偵測到 DDoS 攻擊發生時，系統可以依據偵測到的攻擊數據來決定要配置多少資源去啟動防禦功能。更甚者，若有其他服務處於較空閒的情況，也可以從其他服務那邊借用資源來協助抵禦攻擊。此外，虛擬化的技術讓網路的建置具有更高的擴充性與彈性。因此，許多大型的電信公司，如 AT&T，為了增加彈性、降低成本、提高公司競爭力等考量，已開始要求其供應商開始支援 NFV 的架構 [1]。

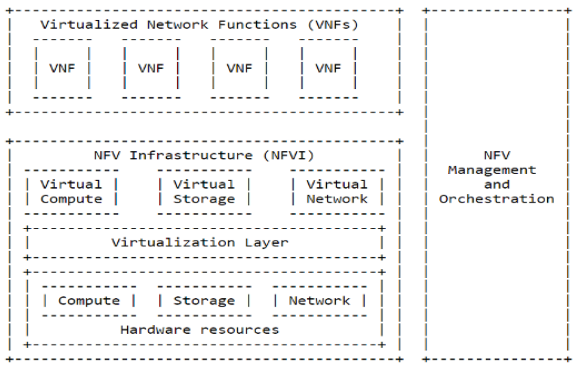

圖 2:ETSI NFV Framework [3]

圖 2 中所顯示的是歐洲電信標準協會 (European Telecommunications Standards Institute，簡稱 ETSI)制定的 NFV 架構，主要由三部分組成，Virtualized Network Function (VNF)乃虛擬化的網路功能，每一個網路服務可以由一個以上的 VNF 組成；NFV Infrastructure (NFVI)則負責將硬體資源虛擬化並提

供給 VNF 使用；至於 NFV Management and Orchestration (NFV MANO)，負責控管 NFV 架構中所有和虛擬化相關的事務(如: 網路服務生命週期、VNFs 生命週期、NFVI 資源管理等)。

3. 文獻探討

在 ETSI NFV 參考架構 [3] 中，NFV MANO 需要管理的事項很多，因此其功能又被細分成三個子功能區塊，其分別是 NFV Orchestrator (NFVO) 負責管理 網路服務的生命週期、VNF Manager (VNFM) 處理 VNF 的生命週期、Virtualized Infrastructure Manager (VIM) 掌管 NFVI 的資源分配。透過這些子功能區塊，我們可以更為精準地去配置 VNF 及調度資源。而 NFV White Paper [4] 提到藉由 NFV 的架構來佈署網路功能有諸多好處，例如：可以根據需求即時建立 VNF、正在運作的 VNF 也能依需求動態地調整資源分配等。我們便以這些特點為基石，聯想到若一網路服務受到攻擊，是否可以運用 NFV 的特性達到自動化佈署防禦機制；並且利用監測系統觀察網路服務的狀態，只在服務受到攻擊時啟動防禦，正常情況則關閉防禦，釋放系統資源。

根據 RFC 4710[5]，使用 Real-time Application QoS Monitoring (RAQMON)架構。在 SIP Server 上以丟包率 (Packet Loss Rate，PLR) [6] 作為 QoS 監測條件，具體公式如下圖: N^{tx} 代表由客戶端 (User Agent) 送出的總封包數；而 N^{rx} 則是由 SIP 伺服器 (SIP Server) 接收到的總封包數。

$$PLR = \frac{N^{tx} - N^{rx}}{N^{tx}} \times 100\%$$

圖 3: PLR 公式

在 NFV 架構下防禦 DDoS，在[7]中可以看到，目前 DDoS 攻擊的防禦方法主要是使用專門的硬體設備所實現的，這種防禦方式無法滿足處理不同類型攻擊的需要，所以 NFV 的靈活性這時就能派上用場。該篇論文中分別使用來源 Source Identification(來源識別)、Rate Limiting(限速)、Signature Filtering(簽名過濾)、Moving Target(移動目標)，來達到防禦目的。

4. 系統架構

4.1 NFV 架構中的 SIP 通訊服務

圖 4 所示為在 NFV 架構下的 SIP 通訊服務架構圖，將 SIP 通訊服務虛擬化成 VNF，並將其佈署在 OpenStack (NFVI) 環境之中。對使用者來說與一般 SIP 通訊服務並無差別，但在重新佈署上，NFV 架構下的 SIP 通訊服務能夠更快的完成佈署[8]。

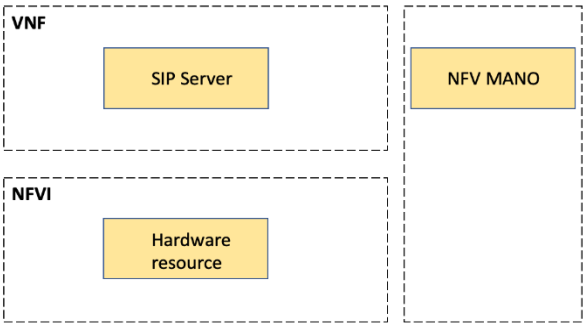

圖 4:NFV 架構中的 SIP 通訊服務

4.2 佈署自動化防禦的 SIP 通訊服務

在圖 4 架構中，雖然依靠 NFV 架構能做到快速佈署，但如遭遇攻擊，並沒有一個偵測及回報系統，仍必須由使用者回報或是管理者發現後，再啟動防禦手段，反應上較為緩慢。圖 5 為增加自動化防禦機制之 SIP 通訊服務。一旦引進自動化防禦機制，則不再需要耗費人力隨時監控系統是否遭到攻擊。在圖 5 中，SIP 通訊服務增加 QoS 偵測系統，偵測 Packet Loss Rate (PLS)。並將 QoS Report 回傳給 NFV MANO。NFV MANO 會進行判斷，一旦 PLS 超過定義值或是 SIP 通訊服務超過一定時間沒有傳送 QoS Report，代表可能遭遇攻擊，則會啟動防禦機制。防禦的手法則是利用 Priority Queue 去實現分流。在架構上會有兩條通道，一條為沒有速率限制的通道，另一條則是有速率限制的通道。一般的用戶在建立連線後，如未有異常情況，會被加入白名單中，此用戶就是使用未有速率限制的通道。一旦被判斷為攻擊者則會被移出白名單，因此攻擊者的流量將被移入有限制傳輸速度的通道中，使攻擊無效，達到防禦手段。

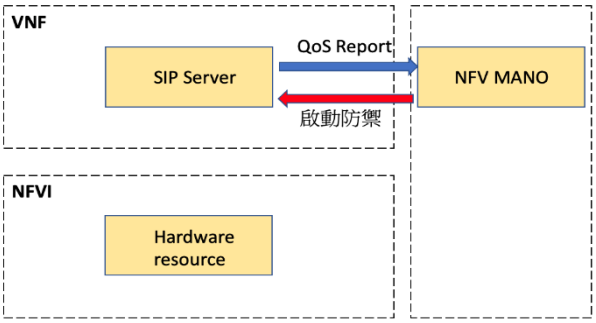

圖 5:增加自動化防禦機制之 SIP 通訊服務

5.系統實作

此節將詳細說明本論文所提自動防禦機制系統之實作細節。

5.1 SIP 通訊服務實現

在網路通訊中電話交換機主機的部分採用 FreeSWITCH 此開源軟體來提供服務。FreeSWITCH 是軟體式電話交換機，支援即時通訊(real-time communication)、網頁即時通訊(Web Real-Time Communication)、Voice over Internet Protocol (VoIP)等多種服務，並因其為開源軟體的特性，支援數十種 Codec，令 FreeSWITCH 具有良好的擴充性，能依使用需求做調整。在本篇論文中，FreeSWITCH 使用版本為 freeswitch-1.10.6，而承載 FreeSWITCH 的主機作業系統則使用 FreeSWITCH 官方建議使用的 Linux Debian 10(Buster)。

5.2 DDoS 攻擊實現

在進行壓力測試時，為了有效率的建立多方擁有不同 IP 位址的攻擊來源，本研究利用 Ansible 與 VM 技術的結合。Ansible 是一款用於自動化佈署的軟體工具，可以遠端配置多台主機、集中下達指令。在數台 VM 組成的叢集中，透過 Ansible control node (可視為叢集的 controller)執行撰寫好的腳本，同時以 Secure Shell 連線並控制多台 VM 作為攻擊方對 SIP 伺服器進行 DDoS 攻擊。

實現 DDoS 攻擊的工具，採用現成的開源封包產生軟體 -- hping3。hping3 最初是由 Salvatore Sanfilippo 開發的開源封包產生器，可以在 Unix-like 的作業系統中讓使用者於命令列直接給予參數並發送封包至指定目標主機，透過查閱官方使用文件[4]可以了解如何迅速產生大量的 TCP 以及 UDP 封包。利用 hping3 進行之 TCP SYN Flooding Attacks，透過傳送大量之 TCP SYN 封包造成目標伺服器無法負荷進而癱瘓服務，其詳細原理可參閱 RFC4987 [5] 以及參考文獻 [11]。

5.3 NFVI 實現

上節有提到 NFV 架構主要由三個部分組成，分別為 NFVI (NFV Infrastructure)、VNFs (Virtualized Network Functions)、NFV MANO (NFV Management and Orchestration)所組成，本節將介紹 NFVI 所使用的工具。

所謂的 NFVI，指的是 NFV 中的基礎建設。主要包含虛擬資源(Virtualized Resources)、虛擬層(Virtualization Layer)、實體資源(Hardware Resources) 這三個區塊。虛擬層介於軟體與硬體(Compute、Storage、Network)之間，跨軟硬體進行整合，並將這些硬體資源進行虛擬化。如此一來，這些資源才能夠讓 NFV MANO 去進行資源的管理，簡單來說 NFVI 就是硬體設備與 NFV MANO 之間的溝通的橋樑。

為了實現 NFV 架構，本論文中使用 OpenStack 軟體進行實作。OpenStack 是美國航空暨太空總署(National Aeronautics and Space Administration ,NASA)以及雲端科技公司 Rackspace 所合作開發的一款開放原始碼軟體。OpenStack 能進行硬體資源的分配以及調度，主要由各種套件所組成，分別為 Nova(運算套件)、Cinder(區塊儲存套件)、Neutron(網路通訊套件)、Keystone(身分驗證套件)、Glance(映像檔管理套件)。有了 OpenStack 就能進行硬體資源的虛擬化整合，並利用這些套件相互協調去滿足 NFV MANO 的需求。

Nova	最核心的部分，主要提供Compute的服務，並管理VM的生命週期。
Cinder	提供儲存服務(Storage service)，為VM建立儲存空間
Neutron	提供OpenStack的網路服務。
Keystone	提供身分認證(Identity Service)的服務。
Glance	負責管理VM的映像檔(Image)。

圖 6: OpenStack 核心套件

5.4 自動化防禦機制

系統啟動之前，先佈署 NFVI 基本環境，如 Router、Network 等，接著透過預先準備好的 SIP VNF Descriptor(VNFD)[17]及 SIP Network Service Descriptors(NSD)[17]，最後是 Software Image，藉此自動化啟動 SIP Service。啟動後在系統運作時，針對 QoS 收集資料並偵測是否有惡意使用者在進行攻擊，流程詳見圖 7。若有偵測到攻擊發生，則自動啟動防禦機制，排除攻擊。期間持續偵測攻擊是否緩解或消失；若攻擊消失後，取消防禦機制，詳見圖 8。

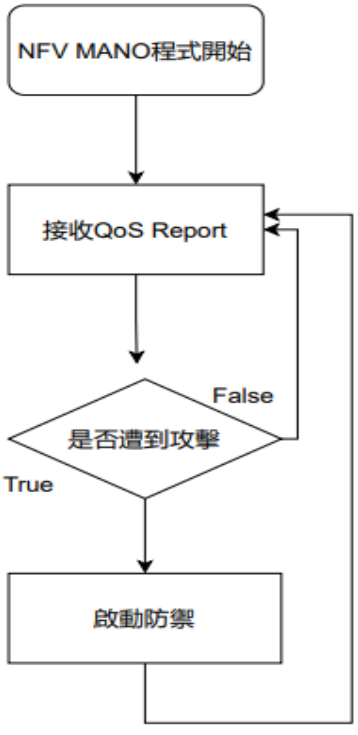

圖 7: 自動化防禦系統流程圖

圖 8:關閉防禦系統流程圖

6. 分析與比較

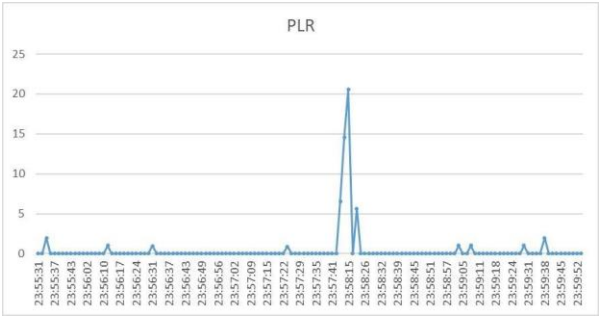

圖 9:Packet Loss Rate(PLR)與時間關係圖

圖 9 是 PLR 與時間關係圖，X 軸是時間，23:55:31 代表為 23 時 55 分 31 秒。Y 軸則是 Packet Loss Rate(PLR)，單位為百分比。

從圖 9 23:55:31 開始是個正常的 SIP 通訊服務，PLR 皆在 5%以內，此為正常值，雖然有些微的 PLR，但是通話不受影響。

在圖 9 23:57:41 開始可以看到 PLR 有了明顯的增加，最高到 20%，通話開始出現音延遲、封包遺失(聲音聽不清楚)等嚴重的影響。此時自動化防禦系統判斷遭受攻擊，自動啟動防禦機制，能夠看到從圖 9 23:58:15 開始 PLR 已開始下降，至圖 9 23:58:26 後回到正常的數值。從遭受攻擊到恢復服務，僅經過 45 秒左右，就讓 SIP 通訊服務回歸正常。以實際案例來看，在 2018 年 GitHub 遭遇 DDoS 攻擊，服務受到影響，GitHub 約 10 分鐘發出警報，最後此次 DDoS 持續約 20 分鐘左右 [9]。相比於 GitHub 遭遇攻擊到排除攻擊，此自動化防禦系統 45 秒內自動回復，可算是十分有效以及迅速。若與傳統的維運模式相比，管理員接到客服電話再去手動啟動防禦，反應時間往往都超過半小時以上，因此整個 SIP 通訊服務的品質就會受到極大的影響。由此可得出結論:自動化防禦機制能成功、迅速且準確的啟動防禦手段。

7. 結論與未來展望

本篇論文證實在 NFV 架構下建立的自動化佈署防護機制。基於系統管理者的角度，此系統架構相對傳統手動啟用防護機制，能更快速地啟用防禦機制，並在攻擊結束後將防禦時所產生的資源占用自動釋放，使系統不會受到任何影響。未來也將會在不同的環境(攻擊強度、網路環境、主機效能)進行相關實驗，使數據更加完整然而本系統目前僅針對分散式阻斷服務攻擊 (DDoS) 進行防護；於服務品質監測層面，亦僅針對封包遺失率 (Packet Loss Rate) 進行監測及處理。於防護服務內容而言，本論文僅探討 VoIP 服務 。未來研究中考慮到上述影響，針對安全，將以複數種防護機制（例如:Load Balance）加入討論，並測試在不同攻擊情境下自動化防護機制的效能；而在服務品質控制的部分，例如 VoIP 服務中，藉由增加服務監測內容，納入延遲 (Latency)、顫動 (Jitter)等指標，來提高實驗數據的精確度；而防禦服務內容的部分，以增加視訊服務為目標，如：以 SIP 為底層架構的 BigBlueButton ，來提高防禦機制的廣度。

致謝

感謝國立暨南國際大學與埔基醫療財團法人埔里基督教醫院產學合作之「埔暨計畫」（110-PuChi-AIR-004)經費補助。

參考文獻

[1] 徐達儒,許鴻基 ,"SDN 與 NFV 相關標準與發展趨勢",Journal of Information and Communication Technology(ICT) No.161 ,15 March 2015.

[2] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol" IETF RFC 3261, June 2002.

[3] A.R. C. J. Bernardos, J. C. Zuniga, L. M. Contreras, P. Aranda and P. Lynch, "Network Virtualization Research Challenges," IETF RFC 8568, April 2019.

[4] M. Chiosi, et. al., "Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & Call for Action," ETSI White Paper,

Oct. 2012.

[5] A. Siddiqui, D. Romascanu,and E. Golovinsky, "Real-time Application Quality-of-Service Monitoring (RAQMON) Framework", IETF RFC 4710, October 2006.

[6] D. Frost and S. Bryant, "Packet Loss and Delay Measurement for MPLS Networks", IETF RFC 6374, September 2011.

[7] Luying Zhou and Huaqun Guo , "Applying NFV/SDN in Mitigating DDoS Attacks ", TENCON 2017 - 2017 IEEE Region 10 Conference,November 5-8 2017.

[8] Alex Su, "The Market Trends and Future Prospects of Network Functions Virtualization" , Journal of Information and Communication Technology(ICT) No.167, October 2016.

[9] Lily Hay Newman ,"GitHub Survived the Biggest DDoS Attack Ever Recorded", WIRED, March 2018. [https://www.wired.com/story/github-ddos-memcached]

[10] Aman Kumar Singh, Raj K Jaiswal, Khakimov Abdukodir, Ammar Muthanna, "ARDefense: DDoS detection and prevention using NFV and SDN" ,12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 5-7 Oct. 2020.

[11] İlker Özçelik and Richard Brooks, "Distributed Denial of Service Attacks: Real-world Detection and Mitigation", CRC Press, 2020.

[12] S.V. Raghavan, E Dawson, "An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks", Springer Science & Business Media, 2011.

[13] Talal Alharbi, Ahamed Aljuhani, Hang Liu, Chunqiang Hu, "Smart and Lightweight DDoS Detection Using NFV", Proceedings of the International Conference on Compute and Data Analysis, pp.220–227, May 2017. [https://doi.org/10.1145/3093241.3093253]

[14] Shang Gao, Zhe Peng, Bin Xiao, Aiqun Hu, Yubo Song, Kui Ren, "Detection and Mitigation of DoS Attacks in Software Defined Networks", IEEE/ACM Transactions on Networking, Vol. 28, No. 3, pp. 1419-1433, June 2020.

[15] K.Munivara Prasad, A.Rama Mohan Reddy, K.Venugopal Rao, "DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms - A Survey", Global Journals Inc. (USA), 2014.

[16] Priyanka Kamboj, Munesh Chandra Trivedi, Virendra Kumar Yadav, Vikash Kumar Singh, "Detection techniques of DDoS attacks: A survey",2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON), 26-28 Oct. 2017.

[17] Shitao Li,John Crandall,"TOSCA Simple Profile for Network Functions Virtualization (NFV) Version 1.0,Committee Specification Draft 04", OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) TC, May 2017.